

**Appendix 2 to
Tenth Amendment of
Master Services Agreement**

May 1, 2015



**Exhibit to Data Center Services
Service Component Provider
Master Services Agreement**

DIR Contract No. DIR-DCS-SCP-MSA-002

Between

**The State of Texas, acting by and through
the Texas Department of Information Resources**

and

Xerox State & Local Solutions, Inc.

**Exhibit 2.6
Network Services
Statement of Work**

May 1, 2015

Change Log

CCR	Amendment	Date	Description
	Amendment 10	May 1, 2015	• Added Section A.5 Port Aggregation Services

TABLE OF CONTENTS

A.0	SERVICE REQUIREMENTS	7
A.1	Common Network Services	7
A.1.1	Physical Scope	7
A.1.2	General Services	7
A.1.3	Network Performance Monitoring and Management Services	9
A.1.4	Network Connectivity and Operations Services	10
A.1.5	Physical Network Environment Services	12
A.1.6	Software Currency and Support Services	13
A.1.7	Network Security Services	13
A.2	Local Area Network (LAN) Services	15
A.2.1	LAN Services – General Requirements	15
A.2.2	LAN Services – Technical Requirements	17
A.3	Remote Access Services	18
A.3.1	Remote Access Services – General Requirements	18
A.3.2	Remote Access Services – Technical Requirements	19
A.3.3	Remote User VPN	19
A.3.4	Remote User VPN (clientless)	20
A.4	Network Appliance Services	20
A.4.1	Network Appliance Services – General Requirements	20
A.4.2	Network Appliance Services – Technical Support	20
A.4.3	Network Appliance Services – Systems Management	21
A.5	Port Aggregation Services	19
A.5.1	Port Aggregation Services – General Requirements	20
A.5.2	Port Aggregation Services – Technical Requirements	20

EXHIBIT 2.6

NETWORK SERVICES STATEMENT OF WORK

Update Methodology to Exhibit 2.6

The following update methodology is incorporated as part of Exhibit 2.6:

Title	Methodology for Updating Exhibit
<u>Exhibit 2.6</u> Network Services SOW	<u>Exhibit 2.6</u> may only be modified by formal amendment, in accordance with <u>Section 21.7</u> of the MSA.

Introduction

Service Provider will provide a solution that supports all of the business processes described in this Statement of Work and its Attachments, and that all Services, unless otherwise specifically stated, are included in the Base Charges.

Service Provider will be responsive to the current and future requirements of DIR and DIR Customers, by proactively anticipating needs, and adjusting Services accordingly within the Base Charges. Requirements for New Services will be handled in accordance with **Section 11.5** of the Agreement and Service Provider will work with DIR to assess the impact of these requirements on DIR's and DIR Customers' operating environment and supported Applications in accordance with the terms of the Agreement.

As of the Commencement Date, the Service Provider will assume responsibility for the operation, management, and support of the Consolidated Data Centers LAN, the legacy portion of the SDC LAN, the Winters Data Center LAN supporting in-scope servers, and associated services such as VPN, Network Intrusion Prevention, Load Balancing, Acceleration and Firewall services.

The Service Provider shall also provide the Services in **Exhibit 2.1.2** including integration with enterprise ITIL Service Management processes, in conjunction with the Services described in this Exhibit.

Service Management

DIR bases its Service Management practices on the ITIL, a world-wide recognized best-practice framework for the management and delivery of IT services throughout their full life-cycle. Accordingly, DIR requires that Service Provider Service Management practices, which are used to support the Services, be based on the ITIL framework and guidance. The primary structure of the requirements in the Statements of Work are based on an ITIL v2 foundation with ITIL v3 guidance in select functional areas (e.g. Request Management and Fulfillment) with the

expectation of migrating towards ITIL v3 progressively as process improvements are incorporated into the Service Management Manual.

Service Provider responsibilities include:

1. Intentionally deploy and actively manage a set of Service Support Processes and Service Delivery Processes that are based on ITIL guidance to enable consistent management of process-driven IT services seamlessly across a variable number of environments and among DCS Service Providers.
2. Ensure that ITIL-based processes effectively integrate with the processes, functions and roles deployed within and used by DIR, DIR Customers and DCS Service Providers.
3. Execute detailed activities and tasks that are common to IT service operation and maintenance according to the guidance set out in the policies and procedures described in **Exhibit 2.1.2**, including the broader guidance provided regarding the ITIL-based Service Management processes.
4. Design processes to enable the effective monitoring and reporting of the IT services in a Multi-Supplier Environment.
5. Ensure that enterprise processes (e.g. Change Management, Configuration Management, Problem Management) are followed across the DCS Service Providers and Third Party Vendor(s) processes.
6. Coordinate the execution of all the processes across the DCS Service Providers, DIR, and DIR Customers in order that all the individual components that make up the IT Services are managed in an end-to-end manner.

A.0 SERVICE REQUIREMENTS

All activities required to provide the Services set forth in this Statement of Work, including project-related support activities, are included in the Charges.

A.1 Common Network Services

A.1.1 Physical Scope

DCS Network shall have the meaning set forth in **Exhibit 1**.

A.1.1.1 Sites

The Service Provider will perform the Services at the Consolidated Data Centers, the legacy portion of the SDC, and the Winters Data Center.

A.1.1.2 Demarcation Boundaries of the Services

The Service Provider will perform the Services within the physical boundaries of the DCS Network, as further depicted in the data room, which describes the typical physical configurations, components, and boundaries of these Network Services.

A.1.2 General Services

A.1.2.1 General Management Services

Service Provider responsibilities include:

1. Act as a single point of contact for the management of the DCS Network including assisting the MSI and other Service Component Providers in resolving Network issues.
2. Develop and implement approved Network strategies in support of DIR's and DIR Customers' business objectives and in accordance with Change Management procedures.
3. Provide Authorized Users, other DCS Service Providers, and designated Third Party Vendors with technical support and advice regarding the proper use and functionality of the DCS Network.
4. Analyze and propose cost-effective DCS Network solution alternatives.
5. Support all telecommunication protocols approved for use by DIR, including proprietary protocols in place as of the Effective Date.
6. Provide telecommunication protocol conversion and translation, as required by DIR and DIR Customers.
7. Provide support for gateway services to and from the DCS Network.

A.1.2.2 General Administration Services

Service Provider responsibilities include:

1. Monitor usage of consumables, as well as ordering and storing consumables for the DCS Network environment (e.g. patch cables, cross connects, transceivers).
2. Administer all DCS Network requirements and activities, including processing change requests.
3. Document all aspects of the DCS Network Services for DIR and DIR Customers, including:
 - 3.1. Design criteria and standards
 - 3.2. Escalation procedures
 - 3.3. Service acceptance procedures
 - 3.4. Topology documentation
 - 3.5. Contact information
 - 3.6. System inventories
 - 3.7. Disaster Recovery Plans (including Technical Recovery Guides)
7. Document operations procedures and services.
8. Update site logs.

A.1.2.3 Planning and Design Services

Service Provider responsibilities include:

1. Develop and propose new or enhanced plans and designs on an ongoing basis and in conjunction with the Long-Range IT Plan, as described in **Exhibit 2.1.2**.
2. Provide plans and design for the following components:
 - 2.1. Overall Network Topology, including the physical and logical layout of the DCS Network.
 - 2.2. Addressing and naming schemas.
 - 2.3. Security compliance.
 - 2.4. Network timing services.
 - 2.5. Optimal communications protocols within the DCS Network as necessary to satisfy DIR's and DIR Customers' business and operational requirements as they evolve over the Term.
 - 2.5.1. Where feasible and as approved by DIR, standardized (nonproprietary) protocols should be used.
 - 2.6. Network Equipment.
 - 2.7. Network Software.
 - 2.8. Network Appliances.
 - 2.9. Transport Services.
 - 2.10. Cabling.

3. Document the criteria and assumptions used to develop plans and designs, including:
 - 3.1. Interoperability considerations and assumptions for all Equipment and Software potentially affected by the DCS Network plans and design, including Equipment and Software used by other DCS Service Provider(s) and use by Third Party Vendors.
 - 3.2. Network bandwidth and/or volume assumptions and projections.
 - 3.3. Expected performance and quality of service based on designs and plans, and minimum performance and quality of service expectations.
 - 3.4. Expected availability, based on designs and plans for redundancy, and minimum availability expectations.
4. Utilize design techniques to appropriately prevent broadcast congestion and outages, including:
 - 4.1. Design segmentation of Equipment, traffic, and design features to sufficiently control and contain traffic levels.
 - 4.2. Design sufficient redundancy and alternative routing to meet the Service Levels and DIR's and DIR Customers' security and service continuity requirements.
5. Work cooperatively with other DCS Service Providers, Third Party Vendors, and DIR to facilitate effective planning and design of the DCS Network.

A.1.3 Network Performance Monitoring and Management Services

A.1.3.1 General Monitoring and Management

Service Provider responsibilities include:

1. Monitor and manage continuous end-to-end performance of the DCS Network, including:
 - 1.1. Monitor the DCS Network at demarcations to be agreed on by DIR to measure, monitor, and report end-to-end performance of the DCS Network.
 - 1.2. Monitor the level and quality of service of the DCS Network for data including monitoring compliance with Service Levels.
 - 1.3. Monitor and manage the DCS Network for service degradation, including detection, isolation, diagnosis, and correction of Incidents on a 24x7 basis.
 - 1.4. Monitor physical and logical connections to the DCS Network.
 - 1.5. Provide all necessary monitoring, diagnostic, and maintenance systems and Software to meet monitoring and management requirements.
 - 1.6. Identify actual and potential bottlenecks that affect the Services.
 - 1.7. Perform necessary daily diagnostic routines.
 - 1.8. Employ element management system tools to monitor events that exceed design thresholds, as well as:
 - 1.8.1. Use the tools to provide automated alarms and indication of DCS Network Incidents when thresholds are exceeded.

- 1.8.2. Integrate the tools to automatically generate an Incident within the Incident Management System, as described in **Exhibit 2.1.2** when thresholds are exceeded.
 - 1.8.3. Develop reporting and corrective action procedures to address when design thresholds are exceeded.
 - 1.8.4. Execute corrective action procedures when design thresholds are exceeded.
2. Notify DIR and DIR Customers of any need for an unscheduled interruption.
3. On at least a monthly basis, report to DIR on DCS Network performance, resource shortages, utilization statistics and trends.
4. Provide an easily accessible service on the Portal to report the operational status of the DCS Network in accordance with the Service Management Manual.

A.1.3.2 Performance Optimization

Service Provider responsibilities include:

1. Optimize and improve the performance and design of the DCS Network using data gathered from performance monitoring and forecasting activities.
2. Perform regular optimization analyses on at least a quarterly basis, and prior to and following any transitions or changes as defined in **Attachment 6-B**.
3. Optimize cost-effectiveness and cost-efficiency, without sacrificing performance or the ability to meet the Service Levels.
4. Use modeling and other analysis tools where applicable to determine methods of improving the performance.
5. Assess and implement alternate methods and procedures to reduce errors and downtime.
6. Develop and deliver optimization plans and schedules acceptable to DIR to address issues identified through trend analysis and standardized reporting.
7. Review optimization activities and progress against plans with DIR on at least a quarterly basis.

A.1.4 Network Connectivity and Operations Services

A.1.4.1 Network Connectivity Services

Service Provider responsibilities include:

1. Obtain approval from DIR prior to establishing or removing Connectivity from the DCS Network to Service Provider Facilities or external networks.
2. Manage and control Connectivity to service demarcations.
3. Provide, manage and operate all Equipment, Software and Cabling for the DCS Network including:
 - 3.1. Configuration.
 - 3.2. Installation.

- 3.3. Testing.
- 3.4. Implementation.
- 3.5. Support.
- 3.6. De-installation.
- 3.7. Verify Connectivity of the Infrastructure and all other directly connected equipment.

A.1.4.2 Transport Support Services

Service Provider responsibilities are for support of DCS Service Providers and DIR Customer Third Parties that provide Transport which connect to the Services in the Consolidated Data Centers and include:

- 1. Provide technical support regarding specific requirements and sizing of Transport.
- 2. Schedule, coordinate, and perform support activities for Transport services, in accordance with schedules approved by DIR, including: installation, testing, support, management, additions, upgrades, changes and deletions.
- 3. Provide Level 2 Support and interface with Level 3 Support as needed for Transport services.

A.1.4.3 Address Management Services

Service Provider responsibilities include:

- 1. Provide address management (e.g. IP) as required by DIR.
- 2. Provide a central support model of management.
- 3. Manage subnets address ranges and overall IP addresses schema.
 - 3.1. Provide address reporting and auditing.
 - 3.2. Provide new address request management services.
 - 3.3. Assign new and existing addresses as required.
 - 3.4. Resolve any address conflicts.
- 4. Administer policies that support consistencies throughout the DCS Network.
- 5. Interface and integrate with other providers of network services (e.g. DNS).
- 6. Appropriately support the delivery of services by other DCS Service Providers and Third Party Vendors.

A.1.4.4 Network Time Services

Service Provider responsibilities include:

- 1. Provide network time source as required.

2. Provide Network Time Protocol (NTP) services to DIR and DIR Customer Networks. The Service Provider will provide DIR with a Stratum 1 time source to synchronize the DCS Network.
3. Ensure all DCS Network Services and systems are using the appropriate (e.g. Stratum 2 or better) network timing source and passing network timing to other services.
4. Make network timing available to other DCS Service Providers.

A.1.4.5 Other Network Operations Services

Service Provider responsibilities include:

1. Develop acceptance test procedures for installation and changes to the DCS Network, and for verifying restoration of availability following problems with the Network.
2. Manage media where appropriate, including off-site storage.
3. Manage the naming, numbering and addressing of all DCS Network components and related configuration items based on schemas approved by DIR, including:
 - 3.1. Document the current naming, numbering and addressing schemas.
 - 3.2. Implement, coordinate, and update new schemas, including developing associated migration plans.

A.1.5 Physical Network Environment Services

A.1.5.1 Site Information and Documentation Services

Service Provider responsibilities within the DCS Network include:

1. Conduct site surveys and document the current physical environment at the site, including:
 - 1.1. Transport and other circuits.
 - 1.2. Network Equipment.
 - 1.3. Demarcation of responsibilities and physical environment comprising the DCS Network (e.g. WAN connections, logical LANs, firewalls).
 - 1.4. Cabling.
 - 1.5. Network points of entry.
 - 1.6. Other relevant environmental requirements and/or attributes that are unique to a site.
2. Document site survey information and asset information in the Asset Inventory and Management System.
3. Maintain current locations lists, network diagrams, inventories, configurations, and other network documentation and information.
 - 3.1. Provide DIR with access to the documentation as requested

A.1.5.2 Cabling Services

Service Provider responsibilities include:

1. Plan, procure, install, operate, administer, maintain, and manage the Cabling within the Service Provider physical demarcation boundaries.
2. Manage cable installations, repairs, and removal using a Software-based cable plant management system where applicable.
3. Document changes to Cabling in the Site survey records, and all changes thereto in the Asset Inventory and Management System.
4. Comply with DIR Cabling standards.
 - 4.1. In the absence of a DIR Standard, use industry standards that meet or exceed local code or other requirements of applicable authorities as approved by DIR.
5. Document, label, and map cable runs in the appropriate Site survey records.
6. Maintain up-to-date cable records where a high concentration of Cabling exists.
7. Inspect and certify cables as required by DIR.
8. Maintain a secure, clean, well-lit, clutter-free Cabling environment in all telecommunications closets and cable plant areas.

A.1.6 Software Currency and Support Services

Service Provider responsibilities include:

1. Interface with other designated Third Party Vendors to promote compatibility of Network Systems, and manage the subcontractors that provide Software support to Services for which the Service Provider is responsible.
2. Fully test all code revisions before their installation on the DCS Network.
3. Proactively notify DIR of availability of new versions of software, including analysis of impact and value of the new version of software. (e.g. fixes and new features applicable to DIR and DIR Customers technical and business environments).
4. Coordinate that production levels are fully supported by Third Party Vendors; maintain a record (for each product in production) of version history and associated availability, as well as of any announced end-of-support or end-of-availability dates.

A.1.7 Network Security Services

Service Provider shall meet the requirements related to physical and logical security set forth in **Exhibit 2.1.2** and in **Exhibit 17**.

Service Provider responsibilities include:

1. Act as a single point of contact for the management of the DCS Network Security Services.

2. Implement and maintain security tools, procedures, and systems required to protect the integrity, confidentiality, and availability of the DCS Network and data on the DCS Network.
 - 2.1. DIR will approve the selection of the security tools.
3. Comply with DIR's and DIR Customers' Network security policies described in **Exhibit 17**, and network architecture and standards, whereby the Service Provider will follow the best practices of either DIR, DIR Customers or Service Provider, whichever requires greater security based on reasonable and prudent standard practices, with approval by DIR.
4. Perform periodic assessments of risk exposure including:
 - 4.1. Gap analyses to indicate exposure to security threats, and report analysis to DIR and DIR Customers as appropriate.
 - 4.2. Action plans to address gaps; integrate actions into Service Provider Problem Management and provide reports to DIR and DIR Customers as appropriate.
 - 4.3. Ratings to gauge progress against closure of gaps.
 - 4.4. Categorize risk in compliance to **Exhibit 17**.
5. Provide data privacy as required by DIR and DIR Customers (e.g. network segmentation, firewalls).
6. Provide access and assist the MSI and DIR's designated Third Party Vendors in performing vulnerability assessments (of the Service Provider supported network infrastructure) upon five (5) day's written notice from the MSI.
7. Perform reactive network security assessments, along with Incident and Problem determination, and in accordance with DIR and DIR Customers security policies.
8. Activate appropriate security monitoring tools, and back up and analyze the logs from these tools, in accordance with DIR and DIR Customers security requirements.
 - 8.1. Manage network security devices in the environment (e.g. NIPS, FW, NIDS) to provide appropriate logging and reporting of network activities.
 - 8.2. Establish working relationships with DIR and DIR Customers as required to ensure that network security elements are configured and functioning properly to meet business needs.
9. Provide recommendations to remediate the gaps identified by analyzing the logs.
10. Utilize Access Control Lists (ACLs) on all networking devices in accordance with DIR and DIR Customers network security policies.
11. Take reasonable and appropriate action designed to prevent unauthorized access to the DCS Network, in accordance with DIR's and DIR Customers' requirements. This will include, where appropriate:
 - 11.1. Use DIR approved security protocols for access for external networks.
 - 11.2. Shut down the Services to prevent further unauthorized access.
12. Monitor usage patterns and investigate and report significant discrepancies in those patterns no later than seventy-two (72) hours after their detection.

13. Report all attempts at illicit monitoring, interception, eavesdropping, toll-fraud or other network security risks to DIR and DIR Customer or its designate when detected or known by the Service Provider.
14. Deliver requested data for DIR's input into a DIR controlled self-assessment process and system.

A.1.7.1 Managed Firewall Services

Service Provider's responsibilities include:

1. Configure and maintain the firewall infrastructure for efficient operation.
2. Maintain the Change Management process approved by DIR for the updating of firewall rules and objects, and obtain proper approvals prior to any revision.
3. Manage and update the firewall rules and objects as required.
4. Respond to incidents and problems with Firewall Services as required.
5. Continuously monitor firewalls, and report any alerts or events to DIR or affected DIR Customers immediately, in accordance with DIR's escalation and reporting procedures.

A.2 Local Area Network (LAN) Services

The Service Provider shall provide LAN Services for the DCS Network, to include the administrative areas within the Consolidated Data Centers that support the delivery of Services.

A.2.1 LAN Services – General Requirements

Service Provider's responsibilities include:

1. Act as a single point of contact for the management of the LAN Services.
2. Develop and implement approved LAN Service strategies in support of DIR's and DIR Customers' business objectives.
3. Provide Authorized Users, other DCS Service Providers and designated Third Party Vendors with technical support and advice regarding the use and functionality of LAN Services.

A.2.1.1 LAN Services – Planning and Design Services

Service Provider's responsibilities include:

1. Assist other DCS Service Providers, DIR and designated Third Party Vendors to analyze the LAN Service equipment and network needs.
2. Provide programming, engineering, and design functions for any proposal requested by the DIR for new equipment or changes to the existing LAN Service environment.

A.2.1.2 LAN Services – Installation, Modification and Removal

Service Provider responsibilities include:

1. Install, change, disconnect or remove LAN Equipment and related Software and configurations to meet DIR's and DIR Customers' business and Application requirements.
2. Implement LAN connections for all Authorized Users, designated Equipment and Applications, other DCS Service Providers and designated Third Party Vendors, as required.
3. Implement LAN segments as required.
4. Implement address ranges as required.
5. Implement routing and filtering as required.
6. Maintain networking environment and upgrade LAN Services as required to meet DIR and DIR Customer business and Application requirements, and in compliance with Refresh targets.

A.2.1.3 LAN Services – Maintenance and Operation

Service Provider's responsibilities include:

1. Where remote operations are not technically and/or economically feasible, perform on-site support for operations as required to meet the Service Levels.
2. Upon DIR or DIR Customer request, provide on-site support as required.
3. Plan, install, operate, and maintain all applicable LAN Services, LAN Equipment, and other network Equipment as assigned by DIR.
4. Manage, maintain and communicate any additions, changes, and deletions.
5. Provide all DIR-requested reports according to the schedules established and documented in the Service Management Manual.
6. Resolve or coordinate the resolution of Network issues, which includes:
 - 6.1. Provide technical information and trouble shooting, and correct programming errors.
 - 6.2. Assist DIR, DIR Customers, other DCS Service Providers, or Third Party Vendors in resolving end user problems.
 - 6.3. Report any potential system problems to the MSI Service Desk and affected DIR Customers.
7. Perform System backups as established in the Service Management Manual.
8. Perform or coordinate all warranty work on all network Equipment.
9. Perform preventive maintenance, including:
 - 9.1. Perform all maintenance according to the manufacturer's specifications.
 - 9.2. Send documentation to DIR to verify that preventive maintenance has been completed.
 - 9.3. Automate manual preventive maintenance tasks by using preventive maintenance systems.

- 9.4. Run maintenance routines prior to each business day.
10. Perform security audits and configuration parameters reviews, and make password changes on all LAN systems at least quarterly.
11. Perform or coordinate all maintenance per the schedule defined in the Service Management Manual and in compliance with Change Management procedures.
12. Perform or coordinate all high-risk maintenance that impacts users on all LAN Services per the schedule defined in the Service Management Manual and in compliance with Change Management procedures.

A.2.1.4 LAN Services – Equipment

Service Provider's responsibilities include:

1. Provide Equipment of the quality and revision levels required by DIR Standards.
2. Test and determine that all Equipment is in compliance with DIR Standards and free of defects.
3. Provide a sparing strategy for parts critical for the operation of the Equipment to meet defined Service Levels.
4. Bring all parts that are repaired up to the current revision level before returning them to the inventory of spare parts.
5. Replace defective parts with parts that are at the current revision level.

A.2.1.5 LAN Services – Monitoring

Service Provider responsibilities include:

1. Configure and activate the appropriate LAN Equipment monitoring.
2. Monitor and manage continuous performance of LAN Systems and LAN Equipment.
3. Use intelligent network devices and systems to effectively monitor LANs remotely.
4. Test LAN Equipment after implementation to include remote monitoring through agents and monitoring systems.
5. Monitor alarms sent by DCS Network Systems, perform emergency and routine service in response to critical and non-critical Incidents.

A.2.2 LAN Services – Technical Requirements

Service Provider responsibilities include:

1. Transport all protocols where it is economically and technically feasible to do so and where there is sufficient capacity to support all traffic and the required Service Levels.
2. Provide DIR and DIR Customers with multi-protocol LANs, including:
 - 2.1. Manage all Layer 3 address spaces, (e.g. IP, and IPX) as well as any and all Layer 2 addressing (e.g. ATM, Frame Relay, SNA, DECnet, and Token Ring LAAs) used to transport LAN traffic.

- 2.2. Manage Application specific network addressing schemas (e.g. VLANs, VRFs, VLAN trunking, X.25 network, Tandem Expand network).
3. Provide Services that comply with applicable open system standards and specifications (e.g. IETF Standard RFCs, ITU-T, ATM forum recommendations, frame-relay forum recommendations, ANSI, and IEEE).
4. Provide secure, encrypted connectivity for Authorized Users to Network services in compliance with the policies and standards of DIR and DIR Customers.
 - 4.1. Employ appropriate encryption measures, such as Triple DES, IPSEC, AES, etc.
 - 4.2. Provide support for Private VLAN to the host and virtual host.

A.3 Remote Access Services

The Service Provider shall provide Remote Access Services for the Consolidated Data Centers.

A.3.1 Remote Access Services – General Requirements

Service Provider's responsibilities include:

1. Act as a single point of contact for the management of the Remote Access Services.
2. Provide for secure and reliable remote access connectivity into Data Center core networks from other DIR networks, DIR Customer networks, the public Internet and other industry standards-based Third Party Vendor networks.
 - 2.1. Facilitate the maintenance of Applications by DIR Customer development staff.
3. Provide mechanisms to meet multiple agency security and Application requirements.
4. Provide a consistent interface to Data Center core networks.
5. Provision Service Requests through consistent online self-service tools.
6. Support the use of common tools (e.g. Portal) for access to user information and administration capabilities.
7. Provide DIR and DIR Customer training and support.
8. Support, manage and operate all remote users access mechanisms.
9. Support, manage and operate solutions for identity and authentication management.
10. Partition the Remote Access Service such that multiple DIR Customers can securely share the Remote Access Service.
11. Support multiple organizations and sub-organization relationships.
12. Support DIR Customer-specified access control policies.
13. Support policy enforcement of access authority.
14. Authorize and restrict access based on multiple factors (e.g. RSA token, certificate, user name, user category, organization, device type and Application).
15. In addition, during any particular implementation, Service Provider will:

- 15.1. Provide project management for all stages of implementation.
- 15.2. Assess current DIR Customer user access policies and configure the platform to support those policies.
- 15.3. Assess DIR and DIR Customer environments to ensure a seamless transition to the solution.
- 15.4. Maintain all current processes and procedures, where ever feasible, to ensure no disruption in user access to secure Applications.
- 15.5. Provide all necessary engineering and services for the design and implementation of policies and authentication mechanisms.
- 15.6. Ensure minimal disruption of service.
16. Provide for proactive monitoring and support.
17. Provide for detailed reporting to meet DIR and DIR Customer audit and compliance requirements.

A.3.2 Remote Access Services – Technical Requirements

Service Provider solution should be designed and implemented to meet the Service Levels, as outlined in **Exhibit 3**, and wherever possible should:

1. Ensure that DIR and DIR Customer's view is of one single platform.
2. Provide a fully redundant network based architecture.
3. Support dynamic routing for better redundancy.
4. Provide for latency based route selection, where traffic is routed to the 'best' network gateway.
5. Avoid the need for dedicated VPN servers and support transparent tunneling.
6. Support NIC registered and RFC1918 addressing schemas.
7. Support fixed IP addressing, such that users receive the same address each time they connect to the network as required.
8. Support split tunneling for single user connections, such that DIR and DIR Customers can access their secure networks and the Internet over a single secure connection.
9. Support use of the Remote Access Services by Third Party Vendors who provide support for Data Center Services via an Internet connection.
10. Provide solutions that are transport and access type independent.

A.3.3 Remote User VPN

Service Provider's responsibilities include:

1. Provide for site-to-site and client-to-site connections that enable fast, reliable and secure access into DIR Customer specified LAN within the Consolidated Data Center.
2. Provide, support, install and manage single-factor and multi-factor authentication mechanisms.

3. Provide, support, install and manage Remote Access Software clients for client-to-site usage.
4. Limit requirements for specialized CPE at the customer premises.

A.3.4 Remote User VPN (clientless)

Service Provider's responsibilities include:

1. Provide secure remote access, including clientless access to authorized web Applications, client/server Applications, and file sharing to DIR and DIR Customers, and designated Third Party Vendors.
2. Allow for authorized access using Internet and DIR WAN connections which require username/password or other credentials for authentication.
3. Ensure the service has no requirements for Software to be installed or maintained on any end-user computing device.
4. Ensure the service has no requirements for specialized equipment at the DIR Customer premises.
5. Enable secure access from public end user computing devices.
6. Enable secure access through firewalls that do not permit IPSec traffic.

A.4 Network Appliance Services

The Service Provider shall provide Network Appliance Services for DCS Networks.

A.4.1 Network Appliance Services – General Requirements

Service Provider's responsibilities include:

1. Provision, install, operate, support, and in all ways manage network based appliances (e.g. network load balancers, in-line intrusion prevention systems, WAN application acceleration systems) as directed by DIR and DIR Customers.
2. Provide and support the use of common tools (e.g. Portal) for DIR and DIR Customers to access user information and provide administration capabilities as required.
3. Provide training and support to Authorized Users.
4. Where reasonably possible provide for the partitioning of the Service such that multiple DIR Customers can securely share the use of Network Appliances, including the support of multiple organizations and sub-organizations.
5. Provide for proactive monitoring and support and in compliance with **Exhibit 2.1.2**.
6. Provide reports on the usage of Network Appliances to support DIR and DIR Customers.
7. Provide additional detailed reporting for auditing and compliance.

A.4.2 Network Appliance Services – Technical Support

Service Provider responsibilities include:

1. Provide all technical system support and reporting for operations including:
 - 1.1. Storage management for all media
 - 1.2. System programming
 - 1.3. Capacity planning
 - 1.4. Performance analysis and tuning
2. Install and maintain all system Software products.
3. Develop and install productivity tools/utilities, and perform all required operational modifications for the efficient and proper delivery of the Services.
4. Provide regular monitoring and reporting of performance, utilization, and efficiency.
5. Provide technical advice and support (e.g. architecture) to the DIR, DIR Customers, DCS Service Providers and specific Third Party Vendors, as required.

A.4.3 Network Appliance Services – Systems Management

Service Provider responsibilities include:

1. Provide, install and utilize tools and processes to allow automated and remote systems management of Network Appliances. Such tools and processes will include:
 - 1.1. Administration, management and configuration
 - 1.2. License management tools
 - 1.3. Performance measurement and tuning
 - 1.4. System monitoring and controls
 - 1.5. Disaster Recovery, Backup, Business Continuity
 - 1.6. Automatic alerting to support automated incident creation and notification of affected DIR Customer
 - 1.7. Configuration discovery
 - 1.8. Patch management

A.5 Port Aggregation Services

Port Aggregation infrastructure gives the Service Provider the ability to forward a copy of the DCS Customer's IP traffic at different points inside the Consolidated Data Center (CDC) to an endpoint that the DCS Customer provides. Traffic segmentation within port aggregation allows Service Provider the ability to forward a DCS Customer only their IP traffic while keeping other DCS Customers' traffic separate and secure. This allows the DCS Customer the ability to perform packet analysis or application troubleshooting. It also affords Service Provider the ability to troubleshoot connectivity issues at different points in the network.

A.5.1 Port Aggregation Services – General Requirements

Service Provider's responsibilities include:

1. Alignment of Port aggregation service to network responsibilities as covered in A.1- A.2;

2. Port aggregation platform installation, maintenance, line-speed packet deduplication and software patching;
3. Initial configuration and ongoing maintenance of DCS Customer traffic segmentation on the port aggregation platform;
4. Provide each DCS Customer up to two dedicated fiber connections per CDC; and
5. Forward a copy of the DCS Customer's IP traffic across these dedicated fiber network connections to an endpoint specified by the DCS Customer.

A.5.2 Port Aggregation Services – Technical Requirements

The DCS Customer is responsible for the following to ensure delivery of the Port Aggregation Services :

1. DCS Customer's endpoint needs to be short range multimode 10Gb or 1Gb network fiber connections.
2. DCS Customer's end device has to be a physical server or appliance. Virtual servers/appliances are not supported at this time.
3. DCS Customer is responsible for supporting maintaining administering, and patching their endpoint device.

A.5.3 Port Aggregation Services – Systems Management

1. System management includes:
 - 1.1 Alignment to system management functions as described above in A.1.3.